DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT **MICROCOMPUTER DATA/INFORMATION SECURITY**	POLICY NO. **302.8**	EFFECTIVE DATE **10/1/89**	PAGE **1 of 1**
APPROVED BY: **Original signed by:** **ROBERTO QUIROZ** Director	SUPERSEDES **103** **7/13/89**	ORIGINAL ISSUE DATE **7/13/89**	DISTRIBUTION LEVEL(S) **1**

PURPOSE

1.1 To protect against unauthorized access as well as accidental or intentional loss, destruction, or misuse of computer data, including sensitive and confidential patient and personnel information.

POLICY

2.1 All Department of Mental Health (DMH) facilities, e.g., bureaus, divisions, and clinics where microcomputer equipment is located shall make all reasonable efforts to safeguard data from accidental or intentional loss, destruction, or misuse of data resources.

2.2 Knowledge of any violation of data security shall be reported immediately to a supervisor for disposition.

2.3 If purposeful violations of the policies occur, disciplinary action, up to and including dismissal, shall be invoked. Civil penalties may also be appropriate.

2.4 The use of “passwords” to control access to the microcomputer system is at the discretion of the Bureau Director, Deputy/Division Chief, Program Head or designee. Contact the MIS Microcomputer Applications Unit (MAU) for assistance in obtaining a password program and developing guidelines for its usage.

2.5 It shall be the responsibility of the Bureau Director, District/Division Chief, or Program Head where the microcomputer is located for implementing, monitoring, and enforcing these policies and procedures on Microcomputer Data/Information Security.

2.6 All DMH facilities with microcomputer equipment shall implement the following list of policies and procedures on microcomputer data/information security controls:

302.9 CONFIDENTIAL AND SENSITIVE INFORMATION ON MICROCOMPUTER SYSTEMS

3.2.10 MICROCOMPUTER DATA STORAGE AND BACK-UP

AUTHORITY

Welfare and Institutions Code, Section 5330
County Fiscal Manual, Section 12.1.3